UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,253	01/18/2001	Jean-Philippe D. Hausler	5330.1	8171

7590   07/19/2004

J. Robert Brown, Esq.
WORSHAM, FORSYTHE & WOOLDRIDGE, L.L.P.
Energy Plaza, 30th Floor
1601 Bryan Street
Dallas, TX 75201-3402

EXAMINER
ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 07/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *10 January 2001*.

2a) ☐ This action is **FINAL**.　　2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-22* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-22* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All　b) ☐ Some * c) ☐ None of:

　　　1. ☐ Certified copies of the priority documents have been received.

　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2.   Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Patent

Pub No. US 2001/0012362 A1, Marzahn.

3.   Regarding claim 1, Marzahn shows a method for encrypting a message,

comprising:

identifying a message to be encrypted, the message having a plurality of

characters (input source file, Marzahn, page 1, col. 2, sec. 0010);

providing an encryption key array (Matrix Array) having a plurality of records,

each record of the encryption key array having a plurality of elements (Marzahn, page 2,

sec. 0015);

associating characters of the message (String Pointer) with the encryption key

array (Marzahn, page 2, sec. 0015); and

generating an encrypted message by storing a value representing the association

of the encryption key array with characters of the message (MAP, Marzahn, page 2, sec.

0015).

4.   Regarding claim 2, Marzahn shows claim 1 above, and further show providing the encryption key includes generating the encryption key such that each element of one of the plurality of records contains value that is unique to the value contained in each other element in the same record of the encryption key array (Marzahn, page 6, col. 2, sec. 0123).

5.   Regarding claim 3, Marzahn shows claim 2 above, and further show wherein associating the characters of the message with the encryption key array includes associating the character of the message with one of the plurality of records within the encryption key array and further associating the character the message with one of the plurality of elements of the associated record of the encryption key array and obtaining the value contained within the associated element (MAP, Marzahn, page 2, sec. 0015).

6.   Regarding claim 4, Marzahn shows claim 3 above, and further show associating the character of the message with one of the plurality of records within the encryption key array comprises:

associating the position of the character within the message relative to other characters of the message with the position of one of the plurality of records within the encryption key array relative to other records of the encryption key array (relative offset, Marzahn, page. 2, sec. 0017); and

associating the character of the message with the position of one the plurality of elements within the associated record of the encryption key array (targeted for replacement, Marzahn, page 2, sec. 0015).

7.   Regarding 5, Marzahn show an method for encrypting and decrypting a message, comprising:

identifying a message to be encrypted, the message having a plurality of characters (input source file, Marzahn, page 1, col. 2, sec. 0010);

generating an encryption key array having a plurality of records, each record of the encryption key array having a plurality of elements (Matrix Array, Marzahn, page 2, sec. 0015) such that each element of one of the plurality of records contains a value that is unique to the value contained in each other element in the same record of the encryption key array (Marzahn, page 6, sec. 0123);

associating characters (String Pointer) of the message with the encryption key (Marzahn, page 2, sec. 0015);

generating an encrypted message storing encrypted characters representing the association of the encryption key array with characters of the message;

associating the encrypted characters of the encrypted message with the encryption key array (MAP, Marzahn, page 2, sec. 0015); and

generating an decrypted message storing a value representing the association of the encryption key array with encrypted characters of the encrypted message (decryption, method, Marzahn, page 2, sec. 0022).

8.   Regarding claim 6, Marzahn shows claim 5 above, and further show associating the characters of the message with the encryption key array comprises:

associating the position of the characters within the message relative to other characters of the message with the position of one of the plurality of records within the encryption key array relative to other records of the encryption key array (offset, Marzahn, page. 2, sec. 0017);

associating the characters of the message with the position of one of the plurality

of elements within the associated record of the encryption key array (targeted for

replacement, Marzahn, page 2, sec. 0015); and

determining the value contained within the associated element (Marzahn, page 2,

sec. 0018).

9.   Regarding claim 7, Marzahn shows claim 6 above, and further show associating

the encrypted characters of the encrypted message with the encryption key array

comprises:

associating the position of the encrypted character within the encrypted message

relative to the other encrypted characters of the encrypted message with the position of

one of the plurality of records within the encryption key array relative to the other records

of the encryption key array; and

associating the encrypted characters of the encrypted message with the position of

one of the unique values contained in one of the plurality of elements within the

associated record of the encrypted key array (Decryption steps, Marzahn, sec. 0022).

10.   Regarding claim 8, see reasoning in claim 1 above.

11.   Regarding claim 9, see reasoning in claim 2 above.

12.   Regarding claim 10, see reasoning for claim 6 above.

13.   Regarding claim 11, Marzahn, show a system for encrypting a message,

comprising:

storage device (hard drive, Marzahn, page 1, sec. 0009);

processor programmed to:

identify a message to be encrypted, the message having a plurality of characters

(input source file, Marzahn, page 1, col. 2, sec. 0010);

provide an encryption key array (Matrix Array) having a plurality of records, each

record of the encryption key array having a plurality of elements (Marzahn, page 2, sec.

0015);

associate characters of the message (String Pointer) with the encryption key array

(Marzahn, page 2, sec. 0015); and

generate an encrypted message by storing a value representing the association of

the encryption key array with characters of the message (MAP, Marzahn, page 2, sec.

0015).

14.   Regarding claim 12, see reasoning in claim 2 above.

15.   Regarding claim 13, see reasoning for claim 6 above.

16.   Regarding claim 14, Marzahn shows claim 13 above, and further show the

processor is firmware (burned into ROM, Marzahn, page 1, sec. 0009).

17.   Regarding claim 15, Marzahn shows claim 13 above, and further show the

processor hardware (Marzahn, page 1, sec. 0013).

18.   Regarding claim 16, Marzahn shows a method for concealing information within

a data file, comprising:

providing a first data file (input file) having a plurality of records (inherent:

records make up the content of a file), each record the first data file having a plurality of

elements (Marzahn, page 1, col. 2, sec. 0010);

providing information having a plurality of elements (inherent to contents of a

file, i.e., each value stored in the file); and

generating a second data file by combining elements of the information with

elements of the first data file such that the first and second data files are substantially

similar (output file, Marzahn, page 1, col. 2, sec. 0010).

19.   Regarding claim 17, Marzahn shows claim 16 above, and further show generating

the second data (Matrix Array) includes associating at least one element of the

information with one of the plurality of records within the first data file and further

associating the element of the information with one of the plurality of elements of the

associated record of the first data file (Marzahn, page 2, sec. 0015).

20.   Regarding claim 18, Marzahn shows claim 17 above, and further show the first

data is a data file selected from a group of data files consisting of an audio file, a video

file, an audio-visual file, and a graphics file, and wherein the second data file is a data file

selected from a group of data files consisting of an audio file, a video file, an audio-visual

file, and a graphics file (input/output files are indifferent to type of data they store,

Marzahn, page 1, sec. 0010).

21.   Regarding claim 19, Marzahn shows claim 18 above, and further show the

information concealed within the data file is an encryption key array (input source file is

encrypted, Marzahn, page 1, sec. 0010).

22.   Regarding claim 20, Marzahn shows claim 17 above, and further show generating

the second data file further includes obtaining a value relative to the association of the

information with the first data file and storing the value in the second data file (separate

output file, Marzahn, page 1, sec. 0010).

23.   Regarding claim 21, Marzahn shows claim 20 above, and further show the first

data is data file selected from a group of data files consisting of an audio file, video file,

an audio-visual file, and a graphics file, and wherein the second data file is a data file

selected from a group of data files consisting of an audio file, video file, an audio-visual

file, and a graphics file (input/output files are indifferent to type of data they store,

Marzahn, page 1, sec. 0010).

Claim Rejections - 35 USC § 103

24.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

25.   Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patent

Pub No. US 2001/0012362 A1, Marzahn in view of Patent No. 6,249,866, Brundrett et al.

26.   Regarding claim 22, Marzahn shows claim 21, but fail to further show the

information concealed within the data file is an encryption key array.

However, Brundrett teaches that the randomly generated FEK 60 [File Encryption

Key] (encryption key array) is itself encrypted with the public key 72 of at least one user,

and stored with the encrypted file 70 in a special EFS attribute called the Data Decryption

Field (DDF) 74 (col. 10, line 10-14).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention to modify Marzahn as per teaching of Brundrett to include an

improved system and method for encrypting data that is integrated into a file system (col.
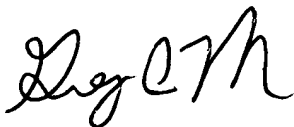
2, line 10-12).

Conclusion

27.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
7/7/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100